A

1. fogalmak  
a, CIA hármas:

* Bizalmasság (Confidentiality): **titkos** **vagy személyes információk** (privacy) **nem kerülhetnek jogosulatlanok kezébe**. **A bizalmasságot** az adatok tárolásánál, feldolgozásánál és továbbításánál is **garantálni kell**.
* Sértetlenség (Integrity):
  + Adatintegritás (data integrity): Teljesülésekor az adat jogosulatlanul **nem módosult** tárolása, feldolgozása vagy küldése során.
  + Rendszer sértetlensége (system integrity): A rendszer működése az elvártnak megfelelő, **jogosulatlan módosításoktól mentes**.
* Rendelkezésre állás (Availability): Biztosítja, hogy a szolgáltatás az arra jogosultak számára a **szükséges időben és időtartamra** használható.

b, Sérülékenység: Az informatikai rendszer olyan **gyengesége**, amelyen keresztül **valamely fenyegetés megvalósulhat**. Rendszerelem módosulhat, szivárogtathat, nem elérhető vagy nagyon lassú.

c, Kártékony program: Olyan program, mely valamely **rendszerbe beépülve** az áldozat adatainak, szoftvereinek **bizalmasságát, integritását, rendelkezésre állását veszélyezteti**, vagy **erkölcsi károkat okoznak**, mert pénz, időt, embert kötnek le.

d, Nulladik napi támadás: Valamely számítógépes alkalmazás olyan sebezhetőséget használja ki, ami még nem került publikálásra, a szoftver fejlesztője nem tud róla, vagy nem érhető még el azt foltozó biztonsági javítás.

2. Hálózati kommunikáció aktív támadásai: Megszemélyesítés, Üzenet visszajátszása, Adat módosítása, Terheléses támadás

3. Fejlett Perzisztens Fenyegetés (APT)? Milyen technikák? Egy példa:   
Fejlett Perzisztens Fenyegetés: a fejlett, perzisztens fenyegetettségek összefoglaló neve. Kiberbűnözés, mely üzleti és politikai célpontokat célozzák meg, többféle behatoló technológia és kártékony program alkalmazásával.  
Technikák: pszichológiai támadás, célzott adathalász e-mail, drive-by-downloads, nulladik napi támadás  
pl: Stuxnet: az első katonai féreg, mely 2010-ben bukott le egy iráni nukleáris erőmű számítógépén.

4. Jellemezze a férgeket! Ismertesse terjedési, rejtőzködési módjait. Két kliens oldali sebezhetőség: A szoftver sérülékenységeit aknázza ki, gazdaprogram nem szükséges, megsokszorozódik. Sebezhetőség: Malvertising: A támadó fizet, hogy hirdetések jelenjenek meg a célpont weboldalakon. A hirdetések kártékony programot tartalmaznak.  
E-mail kliensek bugjainak kihasználása.

5. Mi a zsarolóprogram? Ismertesse fajtáit.

- Fájltitkosító ransomware

- Nem titkosító ransomware

- Böngészőlezáró ransomware

Olyan kártékony program meg lezárja a felhasználó fájljait, blokkolja az áldozat hozzáférését a számítógéphez és az okozott károk visszafordításáért minden esetben váltságdíjat követel. Képesek lehetnek az áldozat érzékeny személyes adatainak megszerzésére, védelmi szoftverek leállítására, megtévesztő figyelmeztetések megjelenítésére és más kéretlen tevékenységekre is. Gyakran drive-by-download útján terjednek.

6. Ismertesse az eltolásos titkosítási sémát.  
P = C = K = Zv, ahol v az abc mérete  
Key: K ∈ Zv véletlenül választott  
Enc: ∀m ∈ Zv esetén EncK (m) = m + K (mod v)  
Dec: ∀c ∈ Zv esetén DecK (c) = c − K (mod v)

7. Definiálja a hash függvényt! Ismertesse a kriptográfiai hash függvény biztonsági elvárásait!

* A hash függvények nem injektívak.
* Az (x,x’) ∈ {0,1}\*x{0,1}\* a H hash függvény egy ütközése, ha x nem egyenlő x’ és h(x) egyenlő h(x’).
* Őskép ellenálló: Adott y ∈ Y értékhez, nehéz olyan x ∈ X értéket megadni, hogy H(x) = y.
* Második őskép ellenálló (gyengén ütközésmentes): Adott x értékhez nehéz olyan x’ értéket találni, hogy x nem egyenlő x’ és H(x) = H(x’).
* Ütközésmentes (erősen ütközésmentes): Nehéz olyan x; x’ ∈ X értékeket találni, hogy H(x) = H(x’)

8. Ismertesse az RSA-FDH digitális aláírási sémát!  
1. Véletlenül választunk két nagy prímet: p, q.   
2. Kiszámítjuk az RSA modulust: n = p · q.  
3. Kiszámítjuk n Euler-féle φ függvény értékét: φ(n) = (p − 1)(q − 1).  
4. Véletlenül választunk egy e egészt, ahol 1 < e < φ(n) és (e, φ(n)) = 1.  
5. Kiszámítjuk: d: 1 < d < φ(n), ahol ed ≡ 1 (mod φ(n)).  
PK = (n, e), SK = d és φ(n), p, q titkos paraméterek  
M = {0, 1} ∗ , S = Zn  
SignSK (m) = H(m) d (mod n) ∀m ∈ M, ahol SK = d,  
H : {0, 1} ∗ → Zn hash függvény

B

1.fogalmak  
a, informatika biztonság: Az informatikai rendszer olyan, a védő számára **kielégítő mértékű állapota**, amely az informatikai rendszerben kezelt adatok **bizalmassága, sértetlensége és rendelkezésre állása**, illetve a rendszerelemek sértetlensége és rendelkezésre állása szempontjából zárt, **teljes körű, folytonos és a kockázatokkal arányos.**  
b, hitelesség: Valaminek a forrása az, amit megjelöltek, és a tartalma az eredeti.

* Felhasználó hitelesítése (Entity Authentication): Az a folyamat, amikor egy entitás meggyőződik egy másik entitás identitásáról.
* Üzenet hitelesítő kód (Message Authentication Code): Egy rövid, fix hosszúságú érték, mely lehetővé teszi az üzenet sértetlenségének és forrásának ellenőrzését, de nem biztosítja a letagadhatatlanságot.

c, kockázat: **A fenyegetettség mértéke**, amely valamely fenyegető tényezőből ered. A kockázat egy **fenyegetés bekövetkezése gyakoriságának** és az ez által okozott kár nagyságának a függvénye.

2. Ismertesse a biztonsági tervezési alapelveket: Jogosultságok minimalizálása, Minimalizálás, Több szintű védelem, Open design, Felosztás, Az egyszerű megoldást válasszuk, Pszichológiai elfogadhatóság

3. Ismertesse a Nyilvános Kulcs Infrastruktúra (PKI) elemeit: Regisztrációs hivatal, Hitelesítő hivatal, Tanúsítványtár

4. Jellemezze a vírusukat! Csoportosítsa a vírusokat célpontjuk és rejtőzködésük alapján! egyes csoportok jellemzői.  
vírus: fertőző mechanizmus: ezzel terjed, indíték: mikor aktiválódik a bűntető rutin, büntető rutin: kárt okozó tevékenység  
célpont szerint: boot vírus, alkalmazásvírus, macrovírus, levelező vírus, összetett vírus  
rejtőzködés szerint: titkosított, lopakodó, polimorf, metamorfózisra képes

5. Mi a zombi és a botnet? Mire használhatóak?  
zombi: A zombi számítógépek hálózatba kötve, koordináltan működhetnek.  
használata: DDoS, Spam, forgalomfigyelés, billentyűzetfigyelés, kártékony programok terjesztése, reklámok elhelyezése, online szavazások/játékok manipulálása  
botnet: olyan hálózatra kapcsolt gépek összessége, amelyek felett átvették az irányítást.  
használata: botneten keresztül zombi gépek használata

6. Ismertesse a permutációs titkosítási sémát:  
A nyílt üzenetet n hosszúságú blokkokra osztjuk. A kulcs egy permutáció. A titkosítás során a kulcs alapján permutáljuk a betűknek megfelelő Zv -beli értéket.   
P = C = Znv , ahol v az abc és n a blokk mérete  
K = {(1, . . . , n) összes lehetséges permutációja}  
Key: π ∈ K véletlenül választott  
Enc: ∀m = (m1, m2, . . . , mn) ∈ Znv esetén  
Encπ(m1, m2, . . . , mn) = (mπ(1) , mπ(2) , . . . , mπ(n) )  
Dec: ∀c = (c1, c2, . . . , cn) ∈ Znv esetén  
Decπ(c1, c2, . . . , cn) = (cπ−1(1) , cπ−1(2) , . . . , cπ−1(n))

7. Adja meg a digitális aláírás fogalmát!  
A digitális aláírási séma egy DS = (Key, Sign, Ver) hármas, ahol

* Key: A Key kulcsgeneráló algoritmus a k biztonsági paraméterre kiszámítja a (PK, SK) kulcspárt, ahol PK nyilvános és SK titkos.
* Sign: A Sign aláíró algoritmus az SK titkos kulcshoz és az m ∈ {0, 1} ∗ üzenetre generál egy s = SignSK (m) aláírást.
* Ver: A Ver ellenőrző algoritmus a PK nyilvános kulcsra, az m üzenetre, és az s aláírásra IGAZ vagy HAMIS értéket ad vissza. IGAZ esetén az aláírás érvényes, HAMIS esetén érvénytelen

8. Ismertesse az RSA titkosítási sémát.  
1. Véletlenül választunk két nagy prímet: p, q.   
2. Kiszámítjuk az RSA modulust: n = p · q.   
3. Kiszámítjuk n Euler-féle φ függvény értékét: φ(n) = (p − 1)(q − 1).  
4. Véletlenül választunk egy e egészt, ahol 1 < e < φ(n) és (e, φ(n)) = 1.  
5. Kiszámítjuk: d: 1 < d < φ(n), ahol ed ≡ 1 (mod φ(n)).  
 PK = (n, e), SK = d és φ(n), p, q titkos paraméterek  
M = S = Zn   
SignSK (m) = md (mod n) ∀m ∈ M, ahol SK = d.   
VerPK (m,s) = TRUE, s e ≡ m (mod n); FALSE, egyébként.  
∀(m,s) ∈ M × S, ahol PK = (n, e).

+

1. Fogalmak

a, Üzenet visszajátszás: A támadó lehallgatja az üzenetet, majd újra elküldi

2. Ismertesse a környezeti fenyegetéseket és az ellenük való védekezéseket!

* Nem megfelelő hőmérséklet és páratartalom:
  + Mérőeszközök segítségével a megfelelő környezetet el lehet érni.
  + Ha az érték túllép a megengedett határon, akkor jelez is.
* Vízkár:
  + Vízérzékelők elhelyezése a padlón és az emelt padlók alatt.
  + Víz esetén automatikusan le kell, hogy kapcsolódjon az áram.
* Por:
  + Ventilátor szűrő karbantartása és a helyiség tisztán tartása.
* Tűz, füst:
  + Tűzjelzők, megelőző intézkedések, tűz oltása
  + Ritkán keletkezik katasztrofális tűz egy jól védett számítógépes helyiségben.
  + Úgy kell a helyiséget kiválasztani, hogy minimális legyen a környezetében keletkező tűz, víz, füst kockázata.
  + Védelmi intézkedések: Közös falak legalább egy óra hosszat tűzállók legyenek.
  + Légkondicionálók úgy legyenek megtervezve, hogy a tüzet ne terjesszék.
  + Gyúlékony anyagokat ne tároljunk a helyiségben.
  + Kézi tűzoltókészülék legyen elérhető, egyértelműen jelezve, és rendszeresen tesztelt.
  + Automata tűzoltó rendszer is legyen telepítve.
  + Tűzjelzők vészjelet adjanak le a helyiségben és külső felügyeletnek is.
  + Főkapcsoló szükséges és egyértelműen jelezve legyen.
  + Menekülési útvonalak ki legyen függesztve.
  + Fontos adatok, dokumentumok tűzálló kabinetben legyenek.
  + Az adatok, programok up-to-date másolata más helyiségben legyen.
  + Biztosítási cégek, tűzoltóság vizsgálja át az épületet.

3. Hátsó ajtó: A program egy titkos belépési pontja, mely lehetővé teszi, hogy a belépési pont ismerője a biztonságos hitelesítés nélkül kapjon hozzáférést.

Programozók legálisan használták a hátsóajtókat program tesztelésre. A hátsóajtók veszélyessé válnak, ha a tisztességtelen programozók illetéktelen hozzáférésre használják.

A védelmi intézkedések szoftverfejlesztésekre és szoftver updatekre irányulnak.

4. Rootkit:

* Egy programcsomag, mely installálása után fedett hozzáférést biztosít, tart fent a már fertőzött géphez adminisztrátori (root) jogosultságokkal. Hátsóajtó hozzáférést biztosítanak trójaiak számára úgy, hogy fontos rendszer fájlokat módosítanak.
* Az operációs rendszer valamennyi funkciójához és szolgáltatásához hozzáférést ad.
* Adminisztrátori jogosultsággal, a támadónak teljes kontrollja van a rendszer felett, felrakhat, módosíthat programokat, fájlokat, processzeket monitorozhat, küldhet, fogadhat hálózati forgalmat és hátsóajtó hozzáférést kaphat.
* A gyökércsomag elrejti ezeket a mechanizmusokat.
* Jellemzői:
  + Perzisztens: A gyökércsomag perzisztens helyen tárol kódot, pl. registry-ben és a kódot a felhasználó részvétele nélkül futtatja le.
  + Memória alapú: Nincs perzisztens kód, tehát újraindítást nem éli túl. Mivel csak a memóriában van, nehezebb detektálni.
  + Felhasználói (user) módú: Felhasználói szinten működik az operációs rendszerben. Lehallgatja az API hívásokat és módosítja kapott választ. (Példa: ha egy alkalmazás egy könyvtár listázását kéri, a lista, amit megkap nem tartalmaz olyan bejegyzéseket, melyek a rootkittal kapcsolatos fájlok beazonosítását segítik.)
  + Kernel módú: A gyökércsomag úgy rejti el jelenlétét, hogy módosítja a kernelt.

5. Hasonlítsa össze a szimmetrikus és aszimmetrikus titkosítási sémákat!

A képen szöveg, Betűtípus, képernyőkép, szám látható

Automatikusan generált leírás

6. Ismertesse az AES titkosító algoritmus lépéseit!

Advanced Encryption Standard (AES):

Rijndael: Joan Daemen, Vincent Rijmen

SE = (Key, Enc, Dec) szimmetrikus titkosítási séma.

P = {0,1}128

C = {0,1}128

K = {0,1}128, k ∈ {128,192, 256}

Key: véletlenül választunk egy K ∈ K

Egy kör: SubByte, ShiftRow, MinColumn, AddRoundkey

Körök száma: k=128,10;

k=196, 12;

k=256, 14.

8. Ismertesse a titkosítási sémákkal szembeni támadásokat!